I claim:

1. A multi-purpose authentication device, comprising:

a main memory;

a processor coupled to access the main memory; and

an access code generating means located in the processor for generating a one-time access code associated with a single user's identity, for correlating authentication protocols with the access codes stored in the memory and for communicating the authentication of the user's access to an external protected resource.

an independent power source operationally connected to the processor.

a communications controller for interfacing to an external processing device.

2. The device of Claim 1, further comprising a smart card coupled to the processor through a controller for generating cryptographic keys, for performing encryption, decryption and signing of the single user for gaining access to the external protected resource.

3. The device of Claim 2, wherein said smart card is provided with a programmable ROM.

4. The device of Claim 3, wherein said programmable ROM is EEPROM.

5. The device of Claim 3, further comprising an auxiliary memory for storing user credentials and a controller for interfacing with external hardware, the main memory, the smart card and the processor.

6. The device of Claim 1, wherein said processor controls operation of the device between an active mode, a standby mode and an "off" mode.

7. The device of Claim 1, further comprising a display screen associated with the processor.

8. The device of Claim 7, wherein said processor controls operation of the display screen for displaying a passcode for a predetermined period of time and for de-activating the display screen upon passage of the predetermined period of time.

9. The device of Claim 1, wherein said processor is operationally connected to a control button for activating the processor and generating the passcode upon demand.

10. The device of Claim 1, wherein said communications controller uses a USB interface

11. The device of Claim 1, wherein said independent power source is a rechargeable battery.

12. The device of Claim 1, wherein said independent power source is a replaceable battery.

13. A multi-purpose authentication device, comprising:

a main memory;

a processor coupled to access the main memory;

an access code generating means located in the processor for generating a one-time access code associated with a single user's identity, for correlating authentication protocols with the access codes stored in the memory and for communicating the authentication of the user's access to an external protected resource;

a non-volatile storage memory coupled to a controller for providing an interface of the processor to the external protected resource; and

a smart card operationally connected to the controller for providing encryption and decryption functions and enabling identity management of the user.

an independent power source operationally connected to the processor

a communications controller for interfacing to an external processing device.

14. The device of Claim 13, wherein said smart card is provided with a programmable ROM.

15. The device of Claim 14, wherein said programmable ROM is EEPROM.

16. The device of Claim 13, wherein said processor is operationally connected to a control button for activating the processor and displaying the one-time passcode upon demand.

17. The device of Claim 13, wherein said power source being de-activated after a pre-determined period of time.

18. The device of Claim 13, wherein said processor is coupled to a display screen for displaying the user's authentication code upon demand.

19. The device of Claim 13, wherein said communications controller uses USB communications interface bus.

20. The device of Claim 13, wherein said independent power source is a rechargeable battery.

21. The device of Claim 13, wherein said independent power source is a replaceable battery.